Protected Health Care Application In Cloud using Ciphertext-Policy Attribute-Based Encryption And Hierarchical Attribute-Based Encryption

I. Sudha, R. Nedunchelian

Abstract: ***Cloud computing is becoming an emerging paradigm to tenuously store and Share the data for users. A personal health record (PHR) could be a health record during which the patient keeps health data and other information associated with the patient's care. There is a great challenge of privacy and confidentiality once patient shares their records of the commercial cloud servers, that results in less secure. In view of the above, this paper proposes a technique which combines attribute based access control model with an expansion of ciphertext-policy attribute-set-based encryption (ASBE) and Hierarchical Attribute-based Encryption allows to store the sanitized data securely in the cloud system and also the original data may be retrieved from the sanitized data with the help of the key provided by the data owner. The experimentation is carried out on the data sets and it provides superior performance efficient and accurate results. PHR system categorizes the users to multi security domains so as to scale back key management quality.***

Index Terms: Cloud Computing, Personal Health Records (PHR), Attribute Based Encryption (ABE), Hierarchical Attribute-based Encryption,Ciphertext-policy Attribute-set-based encryption.

I. INTRODUCTION

The individual wellbeing vault created as a model of patient-focused wellbeing data exchange. A human services administration that allows their clients to make, get to and deal with their records at one spot that outcomes in productive recovery of information. By guaranteeing security, various experts have rights to get to the PHR. In the event of crisis circumstance, the office is taken care of with outside security.

Typically, by presenting PHR administrations for every one of the, few security and protection dangers may stop its broad appropriation. While sharing the individual information record to the outsider server, the patient should recall of their power over their information. From one perspective, however, there are sterile guidelines, for example, the use of late changed HIPAA Incorporation of Business Partners Cloud suppliers are commonly not secured elements. Malicious attackers and fraudsters could center the outsider servers to encourage the private information of the patients. For instance, a representative in the division of Veterans Affairs has taken information from their database of touchy PHI of 26.5 million military veterans, together with their security numbers and medical problems without approval. To ensure protection, there is got the opportunity to have fine-grained information access control that works with semi-confided in servers.

This paper proposes a calculation alluded to as ciphertext-policy attribute-set-based encryption and hierarchical Attribute-based Encryption, that is amazingly effective for secure transmission of restorative information inside the cloud framework, when the crucial information is being moved to the end clients. The principle target of the above proposed calculation has been to ensure the information encryption just by demonstrating the fundamental subtleties to the end clients without uncovering the first information.

II. LITERATURE REVIEW

Antonio Criminisi, Patrick Pérez and Kentaro Toyama [1] Richard S. Surwit, Lyle M. Allen, III, Sandra E. Cummings (2000) proposed "Frameworks, techniques and results of PC programs for observing, analysis and treatment of ailments confined remote patients who investigate checking frameworks of patients with remote ailments of patients are dealt with, analyzed and observed by a focal information handling framework to impart and get information from specific patient observing frameworks, These incorporate accepting and putting away quiet information all through the restorative portion calculation to produce a put away medicinal portion for the patient A focal information preparing comprises of an average measurements calculation, acquiring information for every patient and characterizing the patient's therapeutic remedies, every individual patient, just as changes to sedate data, dose and the treatment is conveyed straightforwardly to a patient or to a patient observing framework.

Marc Edward Chicorel (2001) proposes "The notes of medicinal advancement created by the PC console through a coded language dependent on determination" clarified that a documentation framework on restorative advancement that uses an arranged "language" of codes comprising of under two letters in order, when

Manuscript published on 30 September 2019.
***Correspondence Author(s)**

I. Sudha, Research Scholar, Department of Computer Science and Engineering, Saveetha University, Chennai, Tamilnadu, India.

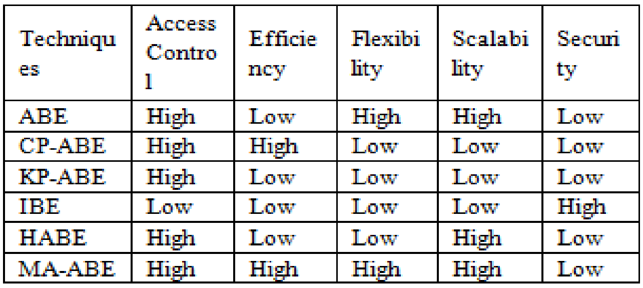
R. Nedunchelian, Professor, Department of Computer Science and Engineering, Karpaga Vinayagar College of Engineering and Technology, Chennai, Tamilnadu, India.

you embed a processor customized in a particular course of action it produces an expressive expression that shows foreordained procedures oftentimes utilized in a specialist's office. Karlyn Jordan (2002) proposed "Wellbeing examination and visualization
of anomalous conditions" by investigating a patient's wellbeing status and entering a scope of the wellbeing enrollment flag, each sign being estimated with the demonstrative default wellbeing capacity is incorporated into the ordinary scope of the patient's wellbeing report, taken at different stages/courses of events.

Jeffrey J. Clawson (2003) has characterized "Strategy and framework for upgrading section procedure of embedding a crisis therapeutic dispatch framework", which investigates a framework created to process, get and react to crisis medicinal calls from crisis dispatchers. Pekka Ruotsalainen (2004) In "A cross-stage model for safe correspondence of electronic medical records" expresses that it is extremely sheltered and secure in sharing the patient's classified data. Roger J. Quay (2005) in "Strategy and contraptions for wellbeing and ailment the executives, which joins the checking of patient information with remote Internet network", clarifies that a capacity that gives a technique to an observing framework remote wellbeing to screen the patient's wellbeing by associating an Internet-empowered remote gadget ("WWD") to a status observing gadget.

J. Bethencourt, A. Sahai and B. Waters (2007) proposed for property based encryption permit scrambled access control where the client's private keys are demonstrated by a lot of properties and a section that encodes the information and can recognize a strategy on these characteristics, which clients can unscramble. It wound up with a moderate loss of productivity in the current frameworks. B. Waters (2011) proposed Cipher content strategy property based encryption. This is extremely expressive, proficient, provable and secure acknowledgment. It additionally gave an execution of the framework, including a few enhancement procedures. Lohr A.R.et.al. (2010) The issues of e-wellbeing mists are capacity of information and the board of e-wellbeing foundation preparing, ease of use and client experience. Protection and security properties have been given to guarantee the essential security in e-human services framework. Dong C et.al., (2010) The server is effective to perform encoded searches and updates in the scrambled information without the learning to the outsiders with the typical content or decoding keys. Li M et.al., (2011) A versatile system for Authorized Private Keyword Search (APKS) on the scrambled information in cloud.P.Saranya (2017), did a study on encryption plans and the subtleties are as per the following

Table 1: Comparison of Encryption Schemes



Techniques	Access Control	Efficiency	Flexibility	Scalability	Security
ABE	High	Low	High	High	Low
CP-ABE	High	High	Low	Low	Low
KP-ABE	High	Low	Low	Low	Low
IBE	Low	Low	Low	Low	High
HABE	High	Low	Low	High	Low
MA-ABE	High	High	High	High	Low

III. METHODOLOGY

The proposed framework coordinates KP-ABE and Multi-Authority ABE and some cryptography plans gives patients have secure sharing of their medical records. Here the primary module examines about attribute based encryption.

A. Registration

Registration used for the few proprietors, AAs and clients. The trait pecking order of the document's leaf hubs is nuclear record classifications, while the inward hubs are compound classifications. PSD information perusers approach the dark box classifications.

Each PSD utilizes two ABE frameworks, the revocable KP-ABE plan is connected for every PUD, our proposed revocable MA-ABE plan is as given underneath.

PUD - public domains
PSD - personal domains
AA - attribute authority
MA-ABE - multi-authority ABE
KP-ABE - key policy ABE

B. Upload files

Upload files with the help of secure keys. Information proprietors transfers the ABR encoded PHR documents, which will be sent to the server. To utilize the transferred records, every one of the information proprietor's PHR documents is scrambled in a particular layout.

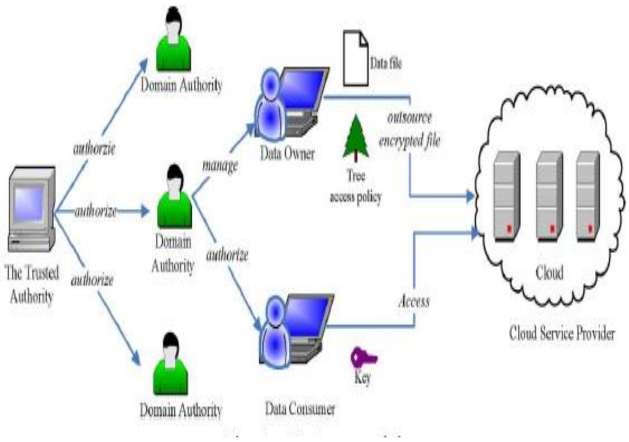


Fig.1. System Architecture

C. ABE for Fine-grained Data Access Control

Attribute based encryption system is connected to acquire the ensured electronic social insurance records and it goes about as a fine-grained access control.This plot fixations basically on how well the properties gets related between the client and data.It manages figure cipher text policy attribute based encryption where the customers can get to the information simply subsequent to be experiencing legitimate approval process. CP-ABE technique is utilized to encode tolerant information utilizing a lot of characteristics and just the clients related to those qualities can decode the ciphertext. The decryption key of every client is related with a lot of properties that procedure the client's authorizations.

Consequently, by guaranteeing the ABE encryption approach the trading of EHR is done in an effective way and the patients medicinal information can be put away to the remote servers.

D. Setup and Key Distribution

This framework utilizes two areas, especially, arrangement and key age. To arrange arrangement, the RSA and Blowfish algorithm are executed utilizing certain parameters. Within the individual area, the framework characterizes various information qualities like profile, patient's restorative history, hypersensitivities, remedies, crisis. Crisis credits are being sketched out to get to the break–glass. The information proprietor makes their customer application through Key-Policy attribute based encryption in this way, making people in general/ace keys. A cloud specialist organization gives the open keys to make encrypted with the help of the framework.

In the public domain, the framework characterizes job characteristics through the secret keys. When a peruser gets to the administration, there exists the entrance benefit and to think of the identical key as far as possible.

E. Encryption

Encryption and decryption pursue an identical standard of CP-ABE with some key qualification. Every factor quality is enhanced with a consistent characteristic. This license greater execution once the arrangement tree contains partner equivalent interest for a variable characteristic. So this upgrade ought to be rejected and an arrangement tree that needs the nearness of the considerable number of qualities that create the parallel worth.

F. Revocation

Revocation alludes to the technique for disavowing the characteristics of the client. This plan performs disavowing utilizing the non-monotonic access structure that appends the requirement of the repudiated clients. A patient-driven model is wanted to share the PHRs during a numerous area and between the multi-authority. The PHR of a patient offers the application level needs between the private and public use.

G. Break-glass module

If there should be an occurrence of crisis, the entrance arrangements should be thus changed. To deal with the case, the information proprietors of PHR should designate the entrance benefit to the crisis division. A break glass access ought to be acquainted with handle the injured individual record. To protect the PHR from vindictive aggressors, the crisis laborers ought to confirm their character and needs to contact the crisis division in order to encourage the brief read keys. When the circumstance is finished, the patient will disavow the rising access.

IV. RESULTS AND DISCUSSION

Usage is the most indispensable stage to accomplish a fruitful framework and to give the client the conviction that the new framework is achievable and successful. Execution of a change to supplant the current one. In the event that there are not very many changes in the framework. It is moderately simple to deal with this sort of discussion. Each program was independently tried at the hour of advancement, utilizing information and it was confirmed that this program was connected to one another as indicated by the particulars of this program, since the client fulfills the PC framework and checks its condition. The PC framework and the earth are tried for client fulfillment. The created framework is acknowledged and demonstrated to be acceptable to the client. In this manner the framework will be actualized soon. A straightforward working method is given with the goal that the client can comprehend the various capacities obviously and rapidly.

In this segment, portray the disambiguation of the element. In this segment each of the screen captures and the graphical UI that the client performs while utilizing CP-ABE and the certain appointment is dissected are introduced.

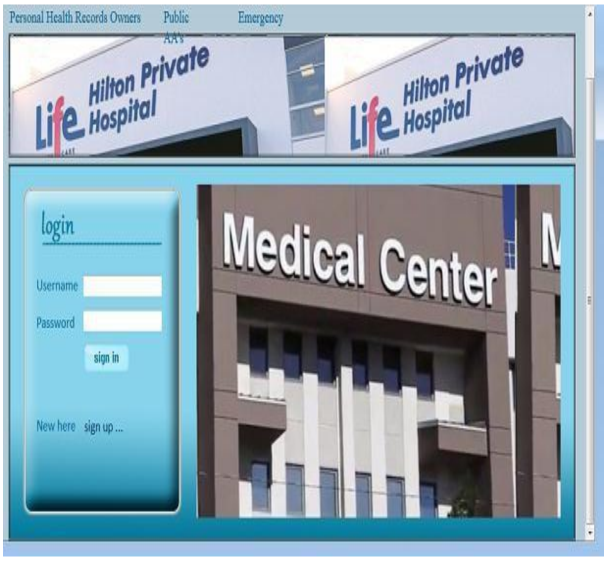
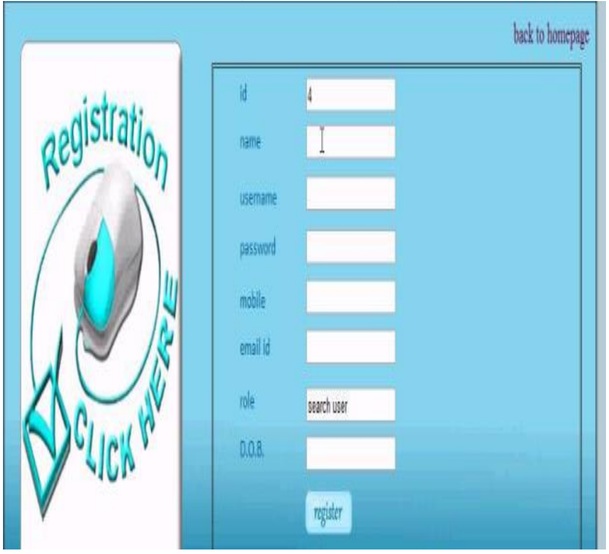
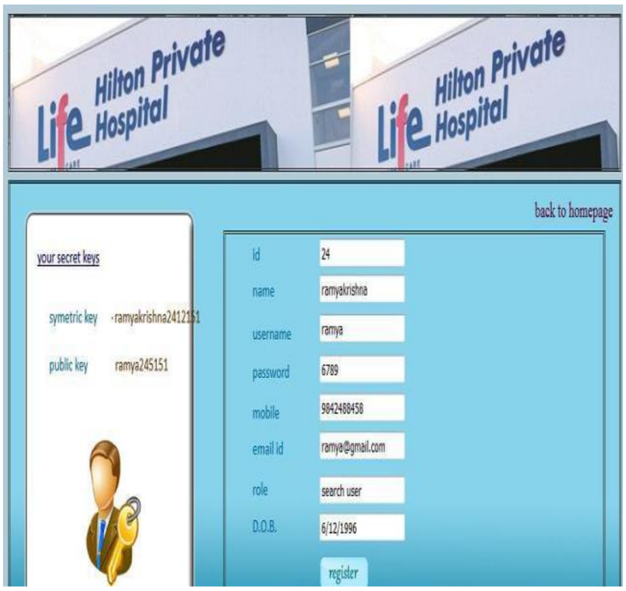

Personal Health Records Owners
Public AA's
Emergency
Life Hilton Private Hospital
Life Hilton Private Hospital
login
Username
Password
sign in
New here sign up ...
Medical Center

Fig. 2. Home page



id 4
name
username
password
mobile
email id
role search user
D.O.B.

Fig. 3. Registration



your secret keys

symetric key ·ramyakrishna2412151

public key ramya245151

id 24

name ramyakrishna

username ramya

password 6789

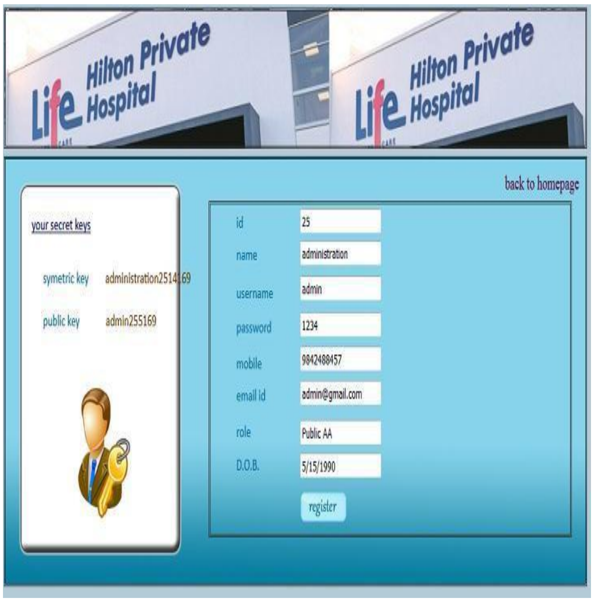
mobile 9842488458

email id ramya@gmail.com

role search user

D.O.B. 6/12/1996

Fig. 4. Setup and Key Distribution



your secret keys

symetric key administration2514169

public key admin255169

id 25

name administration

username admin

password 1234

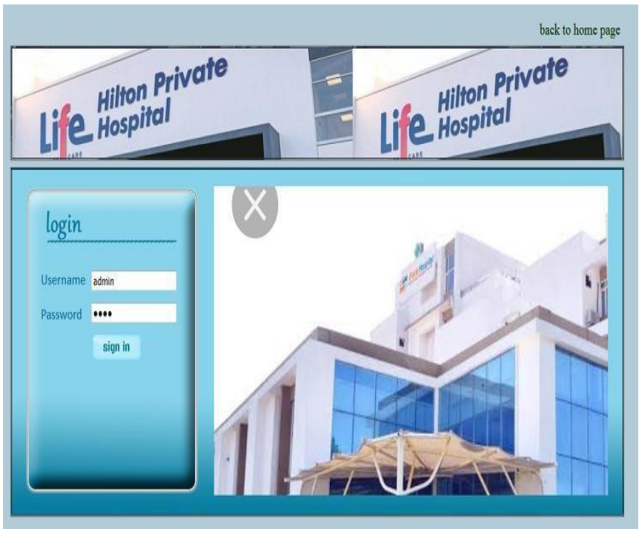
mobile 9842488457

email id admin@gmail.com

role Public AA

D.O.B. 5/15/1990

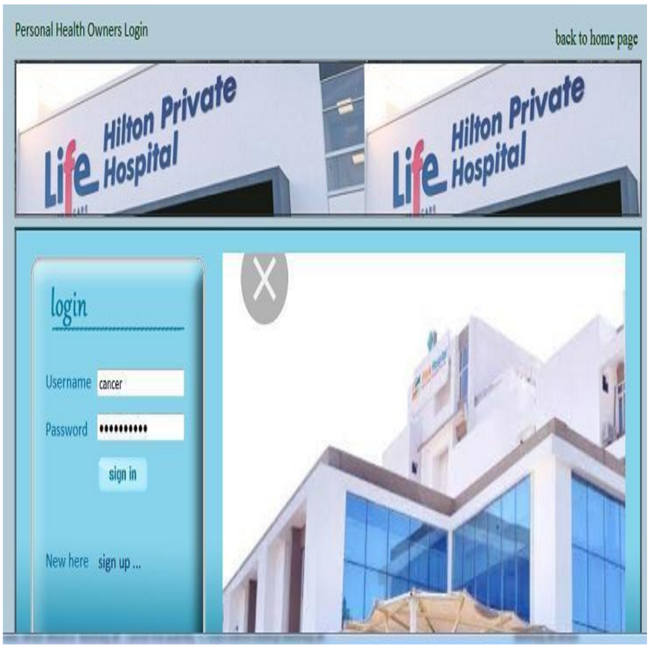
Fig. 5. Public Attribute Authority Registration



Username admin

Password ••••

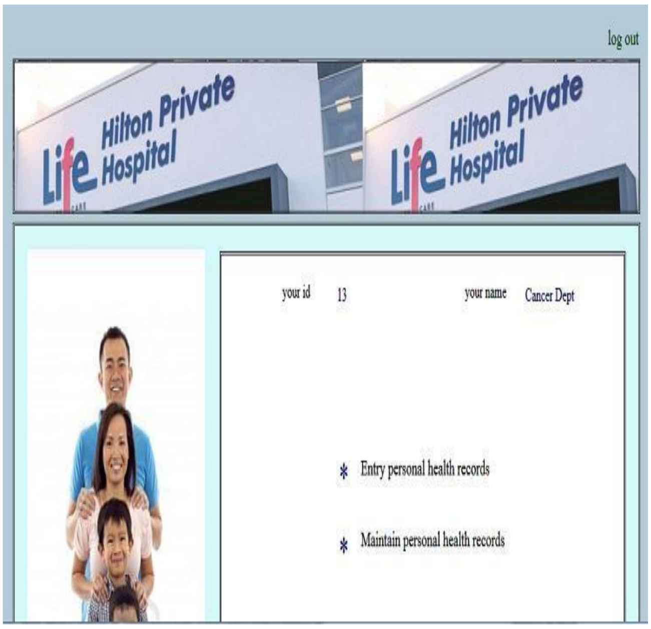
Fig. 6. Public Attribute Authority login


Personal Health Owners Login
back to home page
Life Hilton Private Hospital
Life Hilton Private Hospital
login
sign in
New here
sign up ...

Username cancer

Password ••••••••••

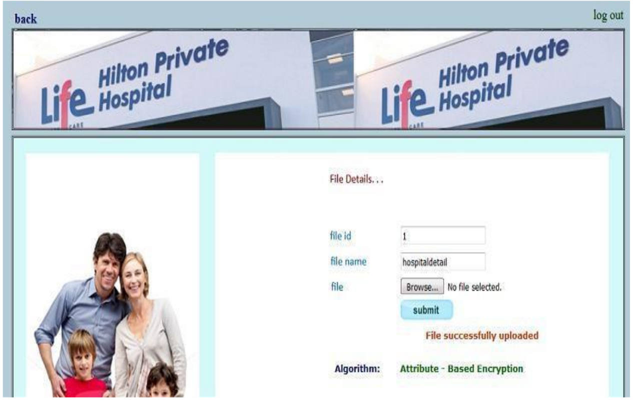
Fig. 7. PHR Owner login



your id 13 your name Cancer Dept

- Entry personal health records
- Maintain personal health records

Fig. 8. PHR Owner After Login



File Details. . .

file id 1

file name hospitaldetail

file Browse... No file selected.

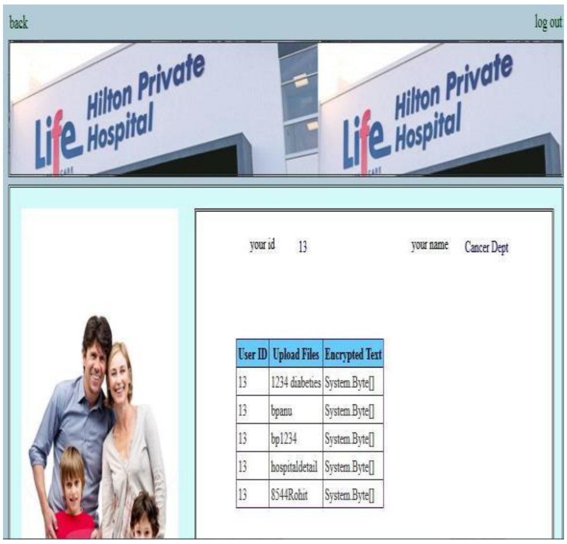
File successfully uploaded

Algorithm: Attribute - Based Encryption

Fig. 9. Upload File

Retrieval Number: K25290981119/19©BEIESP
DOI: 10.35940/ijitee.K2529.0981119
Journal Website: www.ijitee.org

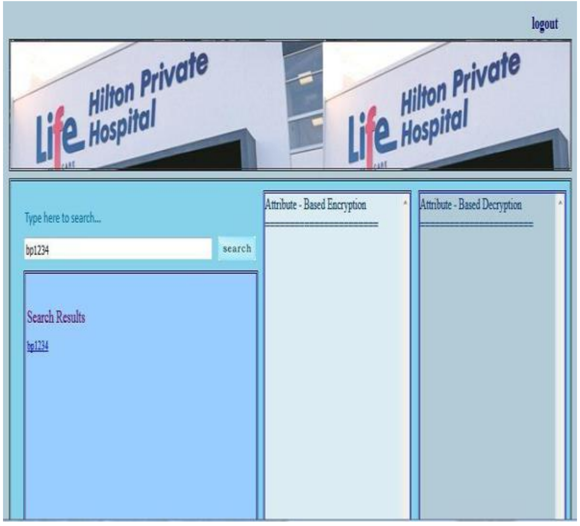
Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



your id 13 your name Cancer Dept

User ID	Upload Files	Encrypted Text
13	1234 diabetes	System.Byte[]
13	bpanu	System.Byte[]
13	bp1234	System.Byte[]
13	hospitaldetail	System.Byte[]
13	8544Rohit	System.Byte[]

Fig. 10. Maintain PHR Information



Type here to search...

bp1234

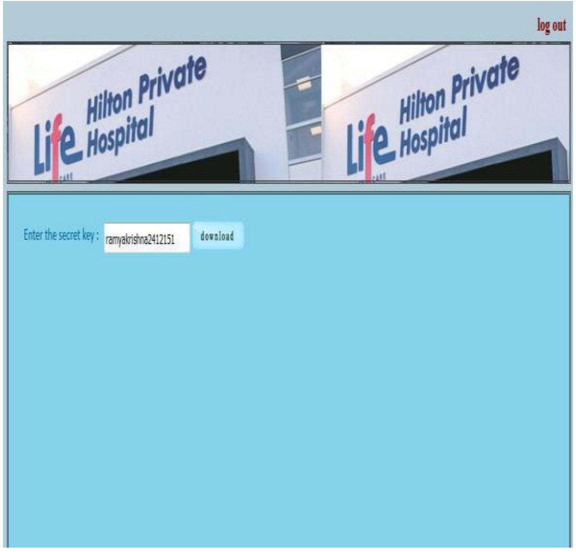
Search Results

bp1234

Attribute - Based Encryption

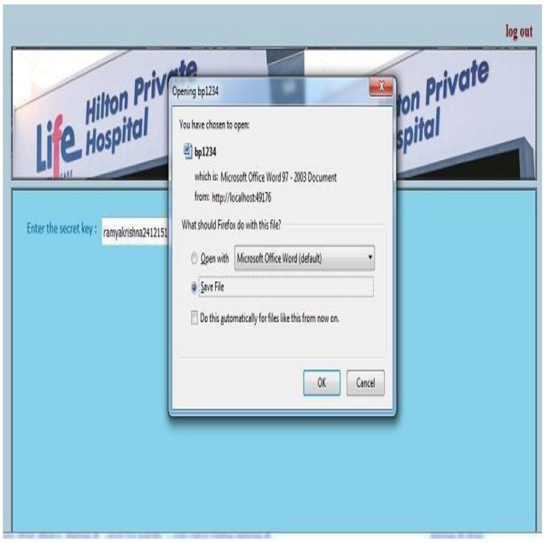
Attribute - Based Decryption

Fig. 11. User Search File



Enter the secret key : ramyakrishna2412151

Fig. 12. User Secret Key



Enter the secret key : ramyakrishna2412151

Opening bp1234

You have chosen to open:

bp1234

which is: Microsoft Office Word 97 - 2003 Document

from: http://localhost:49176

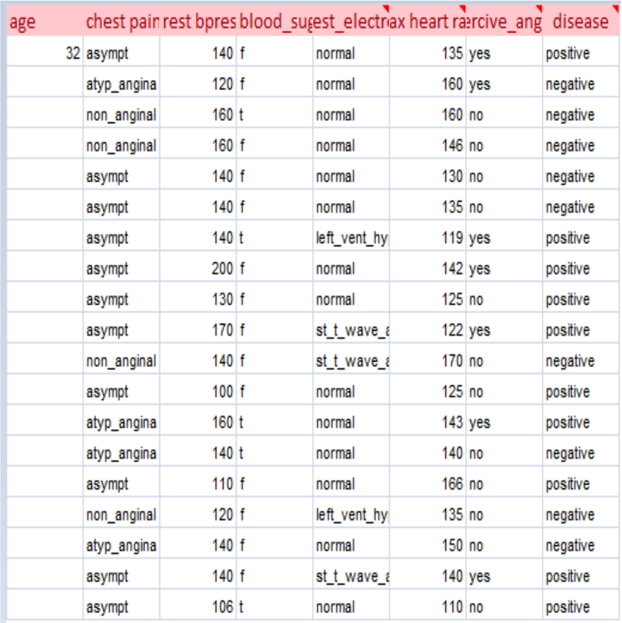
What should Firefox do with this file?

○ Open with Microsoft Office Word (default)

● Save File

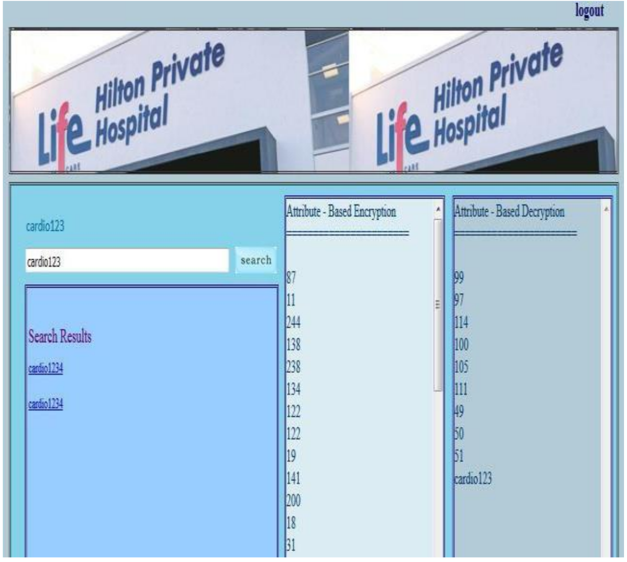
□ Do this automatically for files like this from now on.

Fig. 13. Download File



age	chest pain	rest bpres	blood_su	est_electr	ax heart ra	ercive_ang	disease
32	asympt	140	f	normal	135	yes	positive
	atyp_angina	120	f	normal	160	yes	negative
	non_anginal	160	t	normal	160	no	negative
	non_anginal	160	f	normal	146	no	negative
	asympt	140	f	normal	130	no	negative
	asympt	140	f	normal	135	no	negative
	asympt	140	t	left_vent_hy	119	yes	positive
	asympt	200	f	normal	142	yes	positive
	asympt	130	f	normal	125	no	positive
	asympt	170	f	st_t_wave_a	122	yes	positive
	non_anginal	140	f	st_t_wave_a	170	no	negative
	asympt	100	f	normal	125	no	positive
	atyp_angina	160	t	normal	143	yes	positive
	atyp_angina	140	t	normal	140	no	negative
	asympt	110	f	normal	166	no	positive
	non_anginal	120	f	left_vent_hy	135	no	negative
	atyp_angina	140	f	normal	150	no	negative
	asympt	140	f	st_t_wave_a	140	yes	positive
	asympt	106	t	normal	110	no	positive

Fig. 14. Download File Image



cardio123

cardio123

Search Results

cardio1234

cardio1234

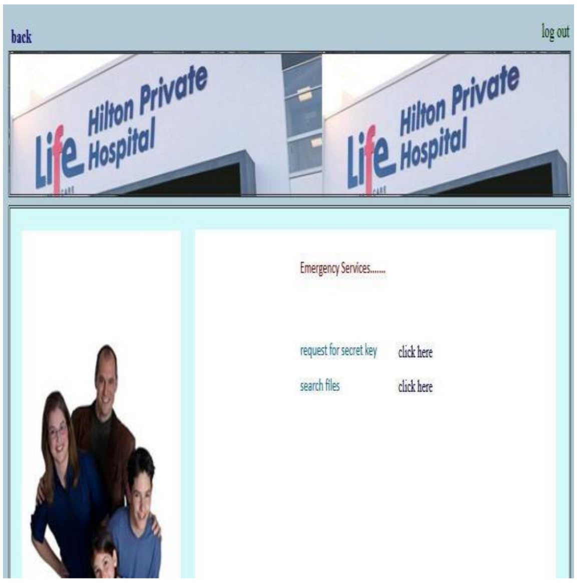
Attribute - Based Encryption

87
11
244
138
238
134
122
122
19
141
200
18
31

Attribute - Based Decryption

99
97
114
100
105
111
49
50
51
cardio123

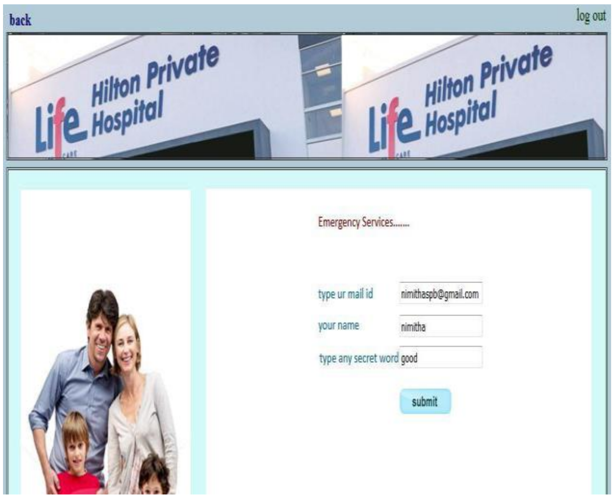
Fig. 15. Encryption and Decryption of the File



Emergency Services.......

request for secret key click here
search files click here

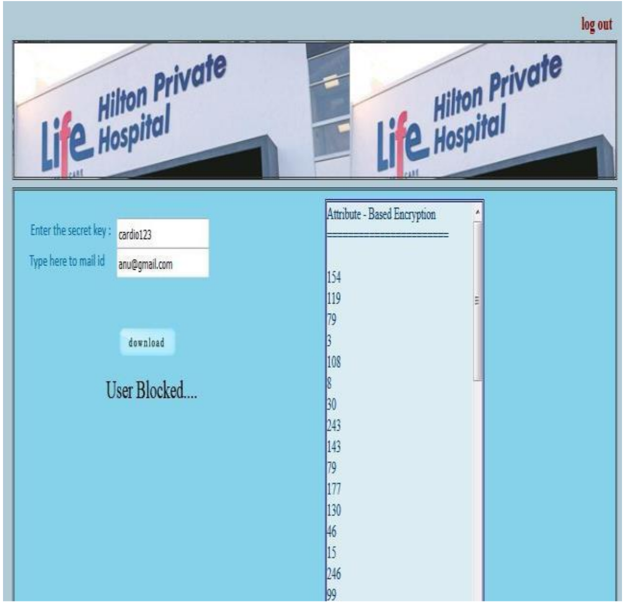
Fig. 16. Emergency Service



Emergency Services.......

type ur mail id nimithaspb@gmail.com
your name nimitha
type any secret word good

Fig. 17. Emergency Service Access Secret Key



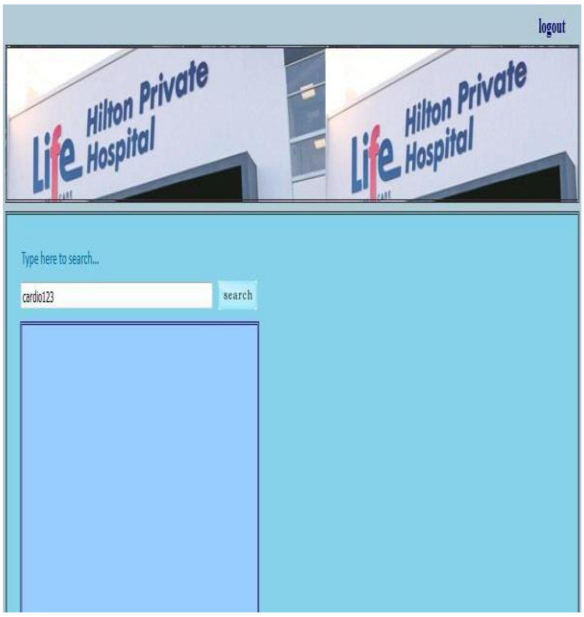
Enter the secret key : cardio123
Type here to mail id anu@gmail.com

User Blocked....

```
Attribute - Based Encryption
============================

154
119
79
3
108
8
30
243
143
79
177
130
46
15
246
99
```

Fig. 18. Emergency Service Access File



Type here to search...
cardio123

Fig. 19. Emergency Service Search Phase

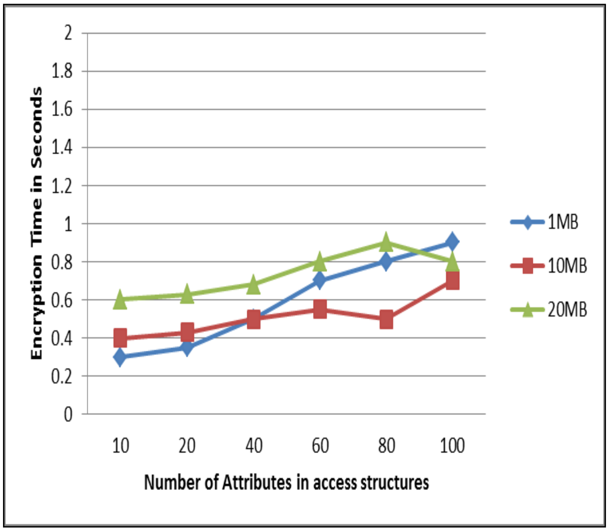


Fig. 20. Encryption time for varying number of attributes in the access structure (Three image sizes)

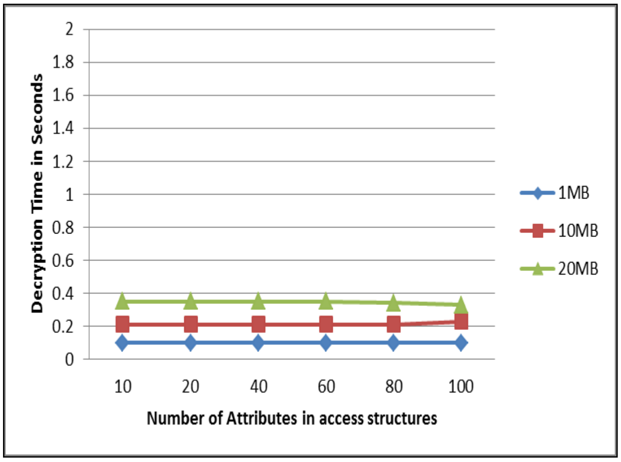


Fig. 21. Decryption time for varying number of attributes in the access structure (Three image sizes)

V. CONCLUSION

This paper illustrates a technique to obtain the protected data using ciphertext-policy attribute-set-based encryption and Hierarchical Attribute-based Encryption. As per this algorithm, the original data are converted into protected data by applying a set of processes and operations for encrypting the data and to show only the essential data for the third parties without revealing the original private data. Further, the data owner can generate a key for retrieving the original data from the sanitized data in the cloud

REFERENCES

1. Saranya, P., Smitha, P. S., Survey on Ciphertext Policy Attribute-Based Encryption (CP-ABE) for Sharing Hierarchical Files. International Journal for Scientific Research and Development. 2017;4(12):46-48.
2. Richard S. Surwit, Lyle M. Allen, III, Sandra E., Cummings 2000 a, Systems, methods and computer program products for monitoring, diagnosing and treating medical conditions of remotely located patients, US6024699 A.
3. Marc Edward Chicorel 2001, Computer keyboard-generated medical progress notes via a coded diagnosis-based language, US6192345 B1.
4. Charlyn Jordan 2002, Health analysis and forecast of abnormal conditions.
5. Jeffrey J. Clawson 2003, Method and system for an improved entry process of an emergency medical dispatch system.
6. PekkaRuotsalainen 2004, A cross-platform model for secure Electronic Health Record communication.
7. Roger J. Quy 2005, Method and apparatus for health and disease management combining patient data monitoring with wireless internet connectivity, US6936007 B2.
8. John Bethencourt, Amit Sahai, Brent Waters, Ciphertext-Policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy(SP '07), Berkeley, CA. 2007;321-334.
9. Hans Lohr, Ahmad-Reza Sadeghi, Marcel Winandy, Securing the E-Health Cloud. Proceedings of the 1st ACM International Health Informatics Symposium(IHI ’10). 2010: 220-229.
10. Dong, C., Russello, G., Dulay, N., Shared and Searchable Encrypted Data for Untrusted Servers. Journal of Computer Security. 2011;19(3):367-397.
11. Li, M., Yu, S., Cao, N., and Lou, W., Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing. Proceedings of the 2011 31st International Conference on Distributed Computing Systems (ICDCS ’11). 2011;383-392.
12. Suhair Alshehri, Stanisław P. Radziszowski, and Rajendra K. Raj, Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption,ACM Digital Library. IJCS. 2011.